BY ORDER OF THE COMMANDER,
51ST FIGHTER WING

AIR FORCE INSTRUCTION 31-601

51ST FIGHTER WING
Supplement 1

15 NOVEMBER 2004

Security

INDUSTRIAL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 51 SFS/SFAI (TSgt Keith W. Elston) Certified by: 51 MSG/CC (Col. Maria J. Dowling)
Pages: 4
Distribution: F

This publication establishes guidance for all Air Force 51st Fighter Wing units which have contractors assigned that handle and use classified materials. This publication implements DoD 5220.22.M, *National Industry Security Program Operating Manual (NISPOM);* AFI 31-401, *Information Security Program Management*; AFI 31-501, *Personnel Security Program Management*; AFI 31-601, *Industrial Security Program Management; AFPD 31-6, Industrial Security; AFI 31-601/*PACAF Supplement 1, AFH 31-602, *Industrial Security Program* and AFI 31-401 51st FW Supplement 1. This publication applies to all assigned, attached, geographically separated units (GSUs), tenant units and staff agencies under the 51 Fighter Wing security program.

AFI 31-601, 22 November 2000, is supplemented as follows:

1.4.1. (Added) Tenant organizations, non-Air Force agencies and 51 FW organizations with internal security offices will exercise physical security supervision of their contracts pursuant to any support agreements or instruction in Block 14 of the DD Form 254, **Contract Security Classification Specification Department of Defense.** The 51 FW/CC retains responsibility and authority for authorizing and/or granting all DoD contractors access to the installation.

1.5.5. The servicing Special Security Office (SSO) at Osan Air Base (OAB) is 7 AF/SSO. As the Senior Intelligence Officer's (SIO) representative, they are responsible for reviewing, approving and granting access to Sensitive Compartmented Information (SCI) portion of the DD Form 254.

1.5.6. The 51st Communications Squadron (51 CS), Information Systems Flight (SCB) is responsible for Automated Information Systems (AIS), Communication Security (COMSEC), Emissions Security (EMSEC) and For Official Use Only (FOUO) programs on OAB.

1.5.6.1. (Added) Coordinate FOUO publications with the FOIA/PA Manager and Staff Judge Advocate (AFI 33-360 V1/PACAF Sup 1, *Air Force Content Management Program--Publications*)

1.5.9.1. (Added) On behalf of the Installation Commander, the 51st Security Forces Squadron (51 SFS/SFAI) is the Servicing Security Activity (SSA) and is responsible for security oversight for classified contracting operations at OAB.

1.6.1.1. The Installation Commander delegates Visitor Group Security Agreement (VGSA) approval to the 51 SFS/CC (ISPM). Additionally, the 51 SFS/CC (ISPM), authorizes contractor operations requiring access to classified information on OAB as either intermittent visitors (less than 90 days) or integrated visitor groups (more than 90 days).

1.6.1.1.1. (Added) Unit security managers will immediately notify the ISPM when DoD contractors work on the installation or at a site within their organization that requires access to classified information/systems.

1.6.1.2. The ISPM will establish a VGSA with integrated visitor groups working on classified contracts.

1.6.1.2.1. (Added) Unit security managers will forward the following information to the ISPM, within five working days of contract performance, for all intermittent contractors working on OAB

1.6.1.2.1.1. (Added) Company name and address

1.6.1.2.1.2. (Added) Contractor type/Classification (e.g., intermittent)

1.6.1.2.1.3. (Added) Duration of contract performance

1.6.1.2.1.4. (Added) Number of employees

1.6.1.2.1.5. (Added) Unit Supported

1.6.1.2.1.6. (Added) Unit Point of Contact or Office of Primary Responsibility

1.6.1.2.2. (Added) Whenever a classified contract on OAB is performed for 90 days or more, the program/project office or the office responsible for initiating or hosting the request for contractor support will forward the following information to 51 SFS/SFAI:

1.6.1.2.2.1. (Added) Name and address of the contractor

1.6.1.2.2.2. (Added) Degree of security clearance required

1.6.1.2.2.3. (Added) Access and storage requirement

1.6.1.2.2.4. (Added) Location of contract performance at OAB

1.6.1.2.2.5. (Added) Name and number of the local senior contract representative

1.6.1.2.2.6. (Added) Contract duration

1.6.1.2.2.7. (Added) Any special security requirements

1.6.1.2.2.8. (Added) A legible copy of the DD Form 254, with attachments (e.g., Statement of Work, etc)

1.6.1.2.2.9. (Added) Copy of the contractors visit request letter

1.6.1.2.2.10. (Added) Name and phone number of sponsoring organization security manager.

1.6.1.4. The 51 SFS/SFAI is the authorized representative to perform industrial security program oversight for on-base contractor operations not placed under Defense Security Service (DSS) cognizance.

1.6.2.4. Upon receipt of the request for review from 51 SFS/SFAI, the program office should take appropriate review actions and issue revisions, as required.

4.1.2. When completing the DD Form 254, coordination with installation security disciplines is required when specialized expertise is warranted for a specific contract. Security disciplines are:

4.1.2.1. (Added) ed) Security Forces, Industrial Security Office (Servicing Security Activity)

4.1.2.2. (Added) ed) 7 AF/SSO for Sensitive Compartmented Information (release & access)

4.1.2.3. (Added) ed) 51 CS/SCB, for COMSEC/EMSEC type information (release & access)

4.1.2.4. (Added) ed) 51 OSS/OSX for OPSEC type information (release & access)

4.1.2.5. (Added) d) The signatures of the Program/Project Manager and Servicing Security Activity (51 SFS/SFAI), in Item 13, Security Guidance. Unit security managers thoroughly review DD Form 254 prior to submission to 51 SFS/SFAI.

4.2. All DD Forms 254 generated by the base contracting office (U.S. Army Contracting Command Korea, 784-5761) for all local contracts administered by USACCK will be coordinated through and reviewed by 51 SFS/SFAI. Additionally, the unit/agency receiving service/support not generated or coordinated by USACCK has the responsibility of coordinating the DD Form 254 through 51 SFS/SFAI for review.

5.3.1. (Added) OAB doesn't have any cleared facilities (cleared facilities are not authorized at overseas locations.)

6.1.1. The ISPM will conduct an annual program review for all Integrated Visitor Groups as part of the sponsoring agencies annual program review IAW AFI 31-401. Unit security managers will ensure Integrated Visitor Groups are included in their semi-annual security self-inspection program. The unit security manager will maintain and provide the ISPM with a copy of the results of the semiannual self-inspections within 30-days of completion and IAW AFI 31-401/51 FW Supplement 1.

7.3.2. The Unit Security Manager via the Senior Contractor Site Representative is responsible for contacting their Facility Security Officer (FSO) and ensuring their Visitor Authorization Letter (VAL) is current at all times. All contractor personnel, including contract personnel without clearances should be in included on all VALs. A current copy signed by the Contractor's FSO needs to be provided to the 51 SFS/SFAI immediately and a copy will also be maintained in their Industrial Security File.

7.3.4. (Added) All integrated contractor personnel via the unit security manager will first in-process through 51 SFS/SFAI for purposes of clearance verification and validation, initial Program Review (PR) scheduling, and records procession prior to performing the terms of their contract. Failure to process through 51 SFS/SFAI could result in untimely delays and potential denial of access to classified, restricted or controlled areas.

9.1.1. COMSEC information or material will not be released to contractors without the approval of the installation COMSEC manager. When a contractor requires access and/or stores COMSEC material or documents, the sponsoring unit will coordinate and obtain approval through the base COMSEC officer. Applicable emission security (EMSEC) clauses will be referenced by the procuring contracting office in DD Form 254, Item 11i. The DD Form 254 will be coordinated with the base EMSEC manager before obtaining ISPM coordination.

9.1.2. Information Assurance offices through unit work group managers will ensure contractors accessing AIS and/or networks that process sensitive but unclassified and classified information will abide by AFI 33-119, *Air Force Messaging*, paragraph 5.3, requirements. Specifically, email addresses must be clearly identified as contractors. Contractor personnel with access to the NIPRNET should be removed from gen-

eral distribution or Plain Language Addresses (PLA), and not given complete access to share drives. They must be restricted from certain folders that do not pertain to the performance of their contract. Contractors will complete all Information Assurance Awareness Program requirements prior to being granted access to the base computer network IAW AFI 33-119, Electronic Mail (E-MAIL) Management and Use**.**

9.1.2.1. (Added) Contractor employees requiring access to classified government AIS networks, or information under the terms of a government contract must have a security clearance. The facility security officer processes these clearances under the NISPOM. Contractor employees who require access to unclassified government information systems require personnel security investigations and trustworthiness determinations processed through their home office in accordance with DoD 5200.2-R, *Personnel Security Program,* AFI 31-501 and AFI 33-119.

9.1.3.1. (Added) IAW AFI 33-119, contractor personnel using unclassified AIS, having access to sensitive information must posses, at a minimum a National Agency Check (NAC) or National Agency Check with Inquiry (ENACI) in accordance with DoD 5200.2-R, or screening in accordance with AFI 31-501. Personnel requiring access to classified systems are subject to the requirements of paragraph **9.1.2.**

10.1. The 7 AF/SSO, Special Security Officer is responsible for direct supervision and oversight of SCI and non-SCI classified information maintained within Sensitive Compartmented Information Facilities (SCIFs).

MAURICE H. FORSYTH, Brigadier General, USAF
Commander